- - Encryption mathematics was expressing the fundamental tenet of the prevailing encryption mode: letter-for-letter in a polyalphabetic fashion. The respective mathematical tool was module mathematics: a mathematical analysis in which any large series of numbers is mapped (matched) to a relatively small, fixed set. Any large as desired integer L is mapped to one of the numbers 1 to n, by dividing it by n, and matching it with the remainder, r:

B1

$$L=k*n+r$$

where k is any integer, and $0 \le r \le (n-1)$. Gauss in 1801 expressed this matching through the congruence symbol (which we shall here use interchangeably with "=", where no confusion may arise).- -

REMARKS

Favorable reconsideration of the present application is respectfully requested in view of the foregoing amendments and the following remarks. Claims 1-5, 7-13, and 16 have been canceled. Claims 17-33 remain pending after the instant amendments.

Objection to the Abstract

Applicant submits that the enclosed Abstract remedies the deficiencies pointed out by the Examiner in the Office Action. The Examiner is respectfully requested to withdraw the objection to the Abstract.

Objection to the Title

The title has been changed to the title suggested by the Examiner. Therefore, the

B

117

Applicant respectfully requests the Examiner to withdraw his objection to the title.

Objections to the Specification

Regarding the Examiner's objection to the use of an undefined character "◊" on page 9, lines 21 and 22, on page 41, line 16, and on page 70 line 5, the Applicant submits that the symbol "<>", and not the symbol "◊", is what is used in the cited pages. Further, because a person of ordinary skill in the art would readily recognize that the symbol "<>" means "not equal", Applicant respectfully submits that there is no need to change that symbol. Therefore, the objection to such use is respectfully requested to be withdrawn.

Regarding the use of the symbol "<=" on page 11, line 24, Applicant has amended the specification as suggested by the Examiner in order to maintain the uniformity of the notation throughout the application. The objection should therefore be withdrawn.

Regarding the objection to the use of "non-standard" notation in connection with Euler's totient function, Applicant respectfully submits that the notation used in the application (i.e., $(b^e)^d$mod n=b) is standard. Referring to equation 12.38 on page 701 of Digital Communications, Fundamentals and Applications, by Bernard Sklar, we find the notation "$X=X^{ed}$ modulo-n". A person of ordinary skill in the art would recognize that $(b^e)^d = b^{ed} = (b^d)^e$. Further, it is also well known in the art that mod n is an abbreviation of modulo-n. For the foregoing reasons the objection to the use of the notation "$(b^e)^d$mod n=b" is respectfully requested to be withdrawn.

Moot Rejections

As a result of the cancellation of claims 1-16, the rejection of claim 1 under 35 U.S.C. §112, first paragraph, is rendered moot. The rejection of claims 1, 4, 7, 9-13, and 16 under 35 U.S.C. §102 as being anticipated by Manual of Cryptohraphy is thus also moot.

Further, the rejection of claims 1-5, 7-13, and 16 under 35 U.S.C. §103(a) as being unpatentable over Gaines is also moot in light of the aforementioned canceled claims. Still further, the rejection of claims 1, 2, 4, 5, and 8 under 35 U.S.C. §103(a) as being unpatentable over Schneier in view of what is well known in the art is also moot.

Rejection of claim 17 under 35 U.S.C. §112, first paragraph

While the Examiner rejected claim 17 for using the symbol *Si*, no correction was requested by the Examiner. Instead, the Examiner correctly assumed that the symbol *Si* denotes a typical symbol of a sequence. Applicant respectfully requests that the Examiner clarify this issue and indicate whether a claim amendment is necessary.

Prior Art Rejection of Claims 17-23

The Examiner rejected claims 17-23 under 35 U.S.C. §103(a) as being unpatentable over Nakamura and Matsui (1987, 1988), hereinafter referred to as "Nakamura", and further in view of what is well known in the art. That rejection is respectfully traversed and withdrawal of the rejection of those claims is earnestly solicited.

Section 2143.03 of the MPEP addresses one of the requirements for properly establishing a *prima facie* case of obviousness. Specifically, that section provides that to establish prima facie obviousness of a claimed invention, all the claim limitations must be taught by the prior art. That section further provides that "[a]ll words in a claim must be considered in judging the patentability of that claim against the prior art."

Applicant submits that claim 17 is not rendered obvious by Nakamura because such reference does not disclose creating a first encryption key by:

"creating a set of vertices, each vertex in the set of vertices being associated with a symbol from said first set of symbols; and defining a relationship for pairs of vertices in the set of vertices, wherein for each pair the relationship is expressed by a vector originating in one vertex and terminating in another vertex, the vector being associated with a symbol from a second set of symbols comprised of So symbols".

Nakamura discloses the use of several random keys to encipher a plaintext (see abstract), which are not created by the method recited by claim 17. Specifically, Nakamura only teaches that the number of encryption keys w_k is equal to n-1 (see page 45), where n is the number of vertices (see page 40) in the graph Gn, and each key w_k is randomly generated (see page 45). Because Nakamura does not use any of the vertices nor any of the links in the graph Gn to create the keys w_k, Nakamura does not teach creating a first encryption key by "creating a set of vertices" and by "defining a relationship for pairs of vertices in the set of vertices, wherein for each pair the relationship is expressed by a vector originating in one vertex and terminating in another vertex" as required by claim 17. In particular, Nakamura teaches connecting all vertices to each other, while in claim 17 the selection of which vertices are connected to which other vertices is part of the key, and is therefore secret.

The Examiner has asserted, however, that "[t]he key itself is a graph (used to transform character links or loops in the dual space)." That assertion, on its face, clearly contradicts the definition of keys w_k as set forth in Nakamura.

Nakamura's algorithm is based on summarizing a numeric value for each closed loop of links on the graph Gn. Nakamura simply proves that the same loop values can be generated by several possible link assignments (of alphabet letters). The keys are then used to select one such other assignment which then becomes the ciphertext. Even if the keys w_k are organized in matrix

B

form to achieve the block code substitution that becomes the ciphertext, the only aspects of that key matrix that remain secret are the keys themselves (i.e., the randomly generated w_k) because Nakamura discloses the exact method to create the matrix parting from the w_k.

By contrast, the present invention as defined by claim 17 requires that the structure of the "graph" remain secret, since "creating a set of vertices" and "defining a [vectorial] relationship for pairs of vertices in the set of vertices" are part of the creation of the key. Because neither the graph Gn nor the matrix constructions disclosed by Nakamura comprise an encryption key, Nakamura does not teach creating a first encryption key by "creating a set of vertices" and by "defining a relationship for pairs of vertices in the set of vertices, wherein for each pair the relationship is expressed by a vector originating in one vertex and terminating in another vertex", as required by claim 17.

Further regarding claim 17, Nakamura fails to associate each vertex in the graph Gn with a symbol from a first set of symbols used to rewrite the plaintext message. Because the symbol assignment for the vertices in claim 17 is part of the key secrecy, and because this aspect of the invention is not disclosed by Nakamura, Nakamura cannot and does not teach all of the limitations of claim 17. For the foregoing reasons, Nakamura does not disclose nor suggest all the elements of claim 17, and therefore, claim 17 is not rendered obvious by Nakamura.

Accordingly, an early indication of the allowability of claim 17 is respectfully requested.

Applicant submits that claims 18-23 are allowable by virtue of their dependency from claim 17. Therefore, the rejection of such claims should likewise be withdrawn.

Prior Art Rejection of Claims 24-27 and 32

The Examiner has rejected claims 24-27 and 32 under 35 U.S.C. §103(a) as being unpatentable over Nakamura and Matsui in view of Gaines.

As discussed above, it is evident that Nakamura fails to teach or suggest expressing a plaintext as a series of vertices and expressing the series of vertices by a sequence of vectors which mark the sequence of vertices. Applicant submits that Gaines fails to cure the deficiencies of Nakamura because Gaines does not disclose the relation among plaintext, vertices and vectors as required by claim 24. Because the combination of Nakamura and Gaines fails to teach all of the claim elements, claim 24 is not rendered obvious by that combination and should thus be allowed. Further, claims 25-27 and 32 should also be allowed at least by virtue of their dependency from claim 24. Accordingly, reconsideration and withdrawal of the rejection of claims 24-27 and 32 is earnestly solicited and an indication of their allowability is respectfully requested.

Rejection of claims 28-31

The Examiner has rejected claims 28-31 under 35 U.S.C. §103(a) as also being unpatentable over Nakamura and Matsui in view of Gaines.

Claim 28 requires "expanding the sequence of symbols by replacing any symbol with an arbitrary number of consecutive appearances of the same symbol." Applicant submits that the Examiner did not address that element in the Office Action and further submits that it is not disclosed by neither Nakamura nor Gaines. Consequently, a *prima facie* case of obviousness has not been established and claim 28 should therefore be allowed. Further, claims 29-31 should also be allowed at least by virtue of their dependency from claim 28. Accordingly, reconsideration and withdrawal of the rejection of claims 28-31 is earnestly solicited and an indication of their allowability is respectfully requested.

Rejection of claim 33

The Examiner has rejected claim 33 under 35 U.S.C. §103(a) as being unpatentable over Nakamura and Matsui in view of Gaines.

Applicant submits that claim 33 should be allowed at least for the reasons set forth above in support of the allowability of claims 17 and 24. Accordingly, reconsideration and withdrawal of the rejection of claim 33 is earnestly solicited and an indication of its allowability is respectfully requested.

Conclusion

As all grounds of objection and rejection have been addressed and overcome, entry of this Amendment and issuance of a Notice of Allowance of the claims now presented, are respectfully solicited.

In the event there are any questions relating to this Amendment or the application in general, it would be appreciated if the Examiner would telephone the undersigned attorney concerning such questions so that prosecution of this application may be expedited. Please charge any shortage or credit any overpayment of fees to Deposit Account No. 23-2185.

In the event that a petition for an extension of time is required to be submitted herewith and in the event that a separate petition does not accompany this response, Applicant hereby petitions under 37 CFR 1.136(a) for an extension of time for as many months as are required to

B

render this submission timely. Any fee due is authorized above.

Respectfully Submitted,

GIDEON SAMID

By: ____________________________
Michael C. Greenbaum
Reg. No. 28,419

The Farragut Building
900 - 17th Street, N.W., Ste. 1000
Washington, D.C. 20006
Telephone: (202) 530-7400
Facsimile: (202) 463-6915

Date: April 11, 2001

B

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE TITLE:

The title has been amended as follows:

A Denial ~~Featured~~ Cryptography Based on Graph Theory

IN THE ABSTRACT:

The currently abstract has been deleted.

A new abstract has been added.

IN THE CLAIMS:

Claims 1-5, 7-13, and 16 have been canceled.

IN THE SPECIFICATION:

Paragraph beginning at page 11, line 17, has been amended as follows:

Encryption mathematics was expressing the fundamental tenet of the prevailing encryption mode: letter-for-letter in a polyalphabetic fashion. The respective mathematical tool was module mathematics: a mathematical analysis in which any large series of numbers is mapped (matched) to a relatively small, fixed set. Any large as desired integer L is mapped to one of the numbers 1 to n, by dividing it by n, and matching it with the remainder, r:

$L=k*n+r$

where k is any integer, and $0\le r\le(n-1)$ ~~0<=r<=(n-1)~~. Gauss in 1801 expressed this matching through the congruence symbol (which we shall here use interchangeably with "=", where no confusion may arise).